



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/288,462	04/08/1999	RICHARD ALEXANDER HARRINGTON	777.222US1	7531

22801 7590 09/25/2002

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER

LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 09/25/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/288,462

Applicant(s)

HARRINGTON ET AL.

Examiner

Benjamin E Lanier

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 April 1999 is/are: a) ☐ accepted or b) ☒ objected to by the ^{draftsperson} Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) ____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

2. The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3. Claims 1, 8-11, 14-16, 19, 20, 22, and 23 are rejected under 35 U.S.C. 102(e) as being anticipated by Yoshida, U.S. Patent No. 6,075,862. Referring to claims 1 and 15, Yoshida discloses a decryption key management scheme for software distribution that allows the re-installation of software without re-acquisition of the decryption key (trigger file) from the software vendor. The decryption key is searched for in a memory device of the user's computer, or acquired from a distribution source of the encrypted software (Internet website) when the decryption key is not found in the memory means. The encrypted software is then decrypted and installed on the user's computer (Abstract).

Referring to claims 8, 14, and 22, Yoshida discloses decrypting encrypted software content (Abstract) stored on a medium such as CD-ROM (Col. 2, lines 12-13).

Referring to claim 9, Yoshida discloses a decryption key management scheme for software distribution that allows the re-installation of software without re-acquisition of the decryption key (trigger file) from the software vendor. The decryption key is searched for in a memory device of the user's computer, or acquired from a distribution source of the encrypted software (Internet website) when the decryption key is not found in the memory means. The encrypted software is then decrypted and installed, by an installer present on the CD-ROM (Col. 5, lines 46-47), onto the user's computer (Abstract).

Referring to claims 10, 11, 19, 20, and 23, Yoshida discloses an installer program (computer-executable instructions) that uses the decryption key if already present, or acquires the key from the software vendor by the communication program (Internet web browser) to decrypt the encrypted software and install the software onto the user's computer (Col. 6, lines 54-64). The decryption key acquired from the software vendor is then stored in the decryption key memory unit as a separate file from the decrypted software content so that even if the decrypted software content is deleted from the hard disk device, the decryption key stored in the decryption key memory unit is maintained therein without being deleted (Col. 7, lines 3-12).

Referring to claim 16, Yoshida discloses a decryption key retrieval program that attempts to retrieve the decryption key for the user's computer in the decryption key memory unit created when the encrypted software has been previously decrypted and installed. If the retrieval program recovers the decryption key then the installer knows that the program has been previously installed. Otherwise the installer must acquire the decryption key from the software vendor (Col. 6, line 54 – Col. 7, line 12).

Art Unit: 2132

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 4, 6, 12, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshida, U.S. Patent No. 6,075,862, in view of Davis, U.S. Patent No. 6,058,478. Referring to claim 4, Yoshida discloses a decryption key management scheme for software distribution that allows the re-installation of software without re-acquisition of the decryption key (trigger file) from the software vendor. The decryption key is searched for in a memory device of the user's computer, or acquired from a distribution source of the encrypted software (Internet website) when the decryption key is not found in the memory means. The encrypted software is then decrypted and installed on the user's computer (Abstract). Yoshida does not disclose encrypted the decryption key. Davis discloses an encrypted public key through the use of a private key (Col. 3, lines 55-59). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the decryption key in the decryption key management scheme of Yoshida in order to authenticate the sender of the information as taught in Davis (Col. 3, lines 60-64).

Referring to claims 6, 12, and 21, Yoshida discloses a decryption key management scheme for software distribution that allows the re-installation of software without re-acquisition of the decryption key (trigger file) from the software vendor. The decryption key is searched for in a memory device of the user's computer, or acquired from a distribution source of the encrypted software (Internet website) when the decryption key is not found in the memory

means. The encrypted software is then decrypted and installed on the user's computer (Abstract). Yoshida does not disclose that the encrypted software module in a cryptographic software module. Davis discloses storing cryptographic programs (Abstract). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the encrypted programs of Davis to be cryptographic programs because there are restrictions on the use and distribution of cryptographic technology, as taught in Davis (Col. 1, lines 31-51), so the decryption key management scheme for software distribution of Yoshida would be ideal to control who has access to these cryptographic programs.

6. Claims 7 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshida, U.S. Patent No. 6,075,862, in view of Davis, U.S. Patent No. 6,058,478 as applied to claims 6 and 12 above, and further in view of Elgamal, U.S. Patent No. 5,825,890. Referring to claims 7 and 13, Yoshida discloses a decryption key management scheme for software distribution that allows the re-installation of software without re-acquisition of the decryption key (trigger file) from the software vendor. The decryption key is searched for in a memory device of the user's computer, or acquired from a distribution source of the encrypted software (Internet website) when the decryption key is not found in the memory means. The encrypted software is then decrypted and installed on the user's computer (Abstract). Davis discloses storing cryptographic programs (Abstract). Davis does not disclose the cryptographic programs being dynamic link libraries (DLL) for providing a secure socket layer (SSL). Elgamal discloses applications that employ a Winsock DLL in conjunction with the SSL library (Col. 12, lines 30-34). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the cryptographic programs of Davis to employ dynamic link libraries in conjunction with a secure

socket layer library in order to achieve a high security communication line in the application program as taught in Elgamal (Col. 12, lines 34-48).

7. Claims 2, 3, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshida, U.S. Patent No. 6,075,862, in view of Easter U.S. 5,563,950. Referring to claims 2, 3, and 18, Yoshida discloses a decryption key management scheme for software distribution that allows the re-installation of software without re-acquisition of the decryption key (trigger file) from the software vendor. The decryption key is searched for in a memory device of the user's computer, or acquired from a distribution source of the encrypted software (Internet website) when the decryption key is not found in the memory means. The encrypted software is then decrypted and installed on the user's computer (Abstract). Yoshida does not describe storing or retrieving the decryption key from a database. Easter discloses a public key that is obtainable from a database (Col. 1, lines 55-58). It would have been obvious to one of ordinary skill in the art at the time the invention was made to store the decryption key of Yoshida in a database so that the software vendor could maintain a central computing system, or key manager, to ensure that each user has their own key as taught in Easter (Col. 1, lines 56-61).

8. Claims 5 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshida, U.S. Patent No. 6,075,862, in view of Easter U.S. 5,563,950 as applied to claim 2, 3, and 18 above, and further in view of Scott, U.S. Patent No. 5,199,073. Referring to claims 5 and 17, Yoshida discloses a decryption key management scheme for software distribution that allows the re-installation of software without re-acquisition of the decryption key (trigger file) from the software vendor. The decryption key is searched for in a memory device of the user's computer, or acquired from a distribution source of the encrypted software (Internet website) when the

Art Unit: 2132

decryption key is not found in the memory means. The encrypted software is then decrypted and installed on the user's computer (Abstract). Easter discloses a public key that is obtainable from a database (Col. 1, lines 55-58). Easter does not disclose generating hash values for each decryption key in the database. Scott discloses generating a hash value from the key value corresponding to database addresses (Col. 1, lines 11-16 & Col. 2, lines 3-10). It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate hash values in the databases of Easter for the decryption keys of Yoshida because the generation of hash values is a technique used in many areas of data processing and data encryption as taught in Scott (Col. 1, lines 11-16).


Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is (703)-305-7684. The examiner can normally be reached on M-Th from 7:30am to 5:00pm, F from 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on (703)-305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703)-746-7239, after final (703)-746-7238, or non-official/draft (703)-746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

BL


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100